D.1 APPROACH SPACING FOR INSTRUMENT APPROACHES (ASIA) 2

D.1.1 ASIA Application Description 2
D.1.2 ASIA Application Requirements Analysis 2
D.1.2.1 ASIA Phases and Processes 5
D.1.2.2 Hazard and Safety Analysis 10
D.1.2.2.1 Operational Hazard Analysis (OHA) 10
D.1.2.2.1.1 Setup: Phase 1 Hazards of ASIA 14
D.1.2.2.1.2 Clearance for Approach Spacing: Phase 2 Hazards of ASIA 15
D.1.2.2.1.3 Conduct Approach Spacing: Phase 3 Hazards of ASIA 15
D.1.2.2.1.4 Completion of Approach Spacing: Phase 4 Hazards of ASIA 16
D.1.2.2.2 Failure-Mode Analysis 16
D.1.2.2.3 Fault Tree Analysis 17
D.1.2.2.3.1 Fault Tree Analysis of Wake Vortex Encounter 19
D.1.2.2.3.1.1 Operational and System Errors Leading to Wake Vortex Encounter Path 20
D.1.2.2.3.1.1.1 Misidentification of Lead Traffic 20
D.1.2.2.3.1.1.2 Misleading Guidance 23
D.1.2.2.3.1.1.2.1 Persistent Misinformation for the Lead Ship 23
D.1.2.2.3.1.1.2.2 Persistent Misinformation for the Trail Ship 25
D.1.2.2.3.1.2 Airborne Separation Violation Alert Fails 26
D.1.2.2.3.1.3 Summary of Wake Vortex Encounter Analysis 29
D.1.2.2.3.2 Fault Tree Analysis of Mid-Air Collision with Lead Aircraft 29
D.1.2.3 Analysis of Requirements Supporting Intended Function of ASIA 33
D.1.2.4 Requirements Summary 34
D.1.2.4.1 Data Requirements 35
D.1.2.4.2 Processing Requirements 35
D.1.2.4.3 Display requirements 35
D.1.2.4.4 Assumptions 36

D.1 Approach Spacing for Instrument Approaches (ASIA)

D.1.1 ASIA Application Description

D.1.2 ASIA Application Requirements Analysis

Working from the OSED contained in Section D.1.1, we now proceed to derive requirements for implementation of ASIA. The requirements analysis process proceeds in several stages; first, we develop requirements derived from the OSED that have implications for the OHA (Operational Hazard Assessment). The requirements are listed in the following tables. Each requirement has an associated unique designator for traceability purposes. After these requirements are listed, we proceed to develop phases and process for ASIA (§D.1.2.1), then conduct the operational hazard analysis (D.1.2.2.1) followed by a failure modes analysis (§D.1.2.2.2), and a fault-tree analysis (§D.1.2.2.3). Requirements that are necessary to support the intended function of the application are contained in §D.1.2.3. Finally, §D.1.2.4 contains a summary of the requirements for ASIA.

The requirements and assumptions from the OSED have been classified into the following categories:

- Operating environment (assumption related to the context of operations), referenced as OExx.
- Operational objective (intended function), referenced as OOxx.
- Operational requirement for the ground segment, referenced as RGxx. Such requirements are to be related to existing ATC procedures and equipment as far as possible; new requirements are derived from the OHA
- Operational requirement for the airborne segment, referenced as RAxx. Such requirements should be related to existing regulations for aircraft equipage or procedures as far as possible. New requirements are derived from the OHA. However, there may be instances when a service is only intended to specific categories of aircraft.
- Selection of technology, referenced as STxx. Allocation for a requirement is already based on an arbitrary technology. Those requirements are kept to a minimum and are generally delayed down to the Allocation of Safety and Operational Requirements phase or even as proposed means of compliance.

Table 1. Operational Requirements and Assumptions Summary

REQ No.	Description	Traceability to paragraph in operations description	Category
OE1	Terminal approach-controlled environment in radar controlled airspace	D.1.1.3	operating environment
OE2	Single stream approach operation under IFR	D.1.1.3	operating environment
OE3	TCAS RA and procedures remain unchanged	D.1.1.6.1	operating environment

REQ No.	Description	Traceability to paragraph in operations description	Category
OE4	The capability to participate in the procedure will initially be indicated in the flight plan	D.1.1.6.1	operating environment
OO1	The ASIA application is an instrument approach procedure involving at least two participating aircraft (i.e., a lead and a trail) and approved instrument approach procedures serving the runways to be used.	D.1.1.6.1	operational objective (intended function)
OO2	The point at which this spacing is achieved will depend upon the differences in final target speeds of the pairs of aircraft involved. However, the minimum wake vortex separation standards are to be maintained throughout the approach.	D.1.1.6.1	operational objective (intended function)
OO3	ASIA application will be designed to function properly in a mixed equipage environment	D.1.1.6.1	operational objective (intended function)
OO4	The length of the final approach will need to be sufficient to ensure adequate distance is available …	D.1.1.6.1	operational objective (intended function)
OO5	Once the aircraft are established on final and the final controller(s) has decided to continue the procedure, the final controller will clear lead aircraft flight crew for ILS for the runway	D.1.1.6.1	operational objective (intended function)
RG1	ATC must pair compatible and eligible aircraft and place them on the final approach course with required separation	D.1.1.6.1	Operational requirement for ground segment
RG2	ATC to determine appropriate equipage of aircraft The feeder controller(s) will know whether the aircraft and flight crew are capable of conducting the procedure by the information provided in the remarks section of the flight strip	D.1.1.6.1 D.1.1.6.1	Operational requirement for ground segment
RG3	On initial contact the feeder controller will instruct the flight crews to expect ASIA	D.1.1.6.1	Operational requirement for ground segment

REQ No.	Description	Traceability to paragraph in operations description	Category
RG4	As soon as possible, but no later than the intercept to the final approach course, the final controller(s) will identify and communicate to the trail aircraft flight crew which aircraft they will be following and its final approach speed	D.1.1.6.1	Operational requirement for ground segment
RG5	Operational procedures for ATC	D.1.1.6.2.1	Operational requirement for ground segment
RA1	Commercial and business jets (FAR/JAR25 and FAR/JAR23)	D.1.1.3	Operational requirement for airborne segment
RA2	Both aircraft in pair must be properly equipped		Operational requirement for airborne segment
RA3	Prior to entering the terminal area, flight crews will have listened to the destination airport ATIS and determined that ASIA in conjunction with the instrument approaches is being used	D.1.1.6.1	Operational requirement for airborne segment
RA4	The flight crew of the trail aircraft must enter the final approach speed of the lead aircraft as well as the desired interval	D.1.1.6.1	Operational requirement for airborne segment
RA5	The trail aircraft flight crew is expected to fly the speed assigned by the final controller until cleared for the approach and the ASIA tool set becomes engaged.	D.1.1.6.1	Operational requirement for airborne segment
RA6	ASIA tool has logic features before engaging speed commands provided by ASIA algorithm. ASIA separation alert to flight crew. No entry of final approach speed disables further processing.	D.1.1.6.1	Operational requirement for airborne segment
RA7	Flight crew of trail a/c expected to follow speed commands of ASIA algorithm Operational procedures for flight crews and airlines operations	D.1.1.6.1 D.1.1.6.2.2 D.1.1.6.2.3	Operational requirement for airborne segment
ST1	At least the trail aircraft must be equipped with ADS-B and ASIA display supported by GPS (or required navigation accuracy, integrity and availability)	D.1.1.6.1	selection of technology

D.1.2.1 ASIA Phases and Processes

Operations supporting the ASIA approach spacing application described in sections X.X can be grouped into four distinct phases (P1 – P4); these are:

P1 Setup for approach spacing procedure
P2 Clear for approach spacing procedure
P3 Conduct approach spacing procedure
P4 Complete approach spacing procedure.

These phases are illustrated in the activity diagram shown in Figure 1 below, along with the specific responsibilities of both the flight crews and air traffic control.

Phases are further subdivided into "processes," that are shown in the process diagram of Figure 2. A large rectangular block depicts each phase; the smaller rectangular blocks represent the processes of each phase. The processes are considered "atomic" in that careful analysis of failures of the processes is expected to assure the safety of the operation.

The setup phase (P1) consists of 8 processes, 7 of which are directly linked. The "ATC Assure Separation" process is a continuous process, based on ATC surveillance using secondary radar, and is independent of the ADS-B surveillance used in the air-to-air parts of the operation.

Process 1.1 (P1.1) consists of ATC providing typical vectors to an ILS approach. The flight crew prepares as usual for final approach and landing, and performs the additional step of entering own ship's planned final approach speed into the approach spacing system through the CDTI user interface (P1.2).

In P1.3 ATC provides a call out for the traffic to be followed (TTF) by the flight crew. The traffic must be identified and selected on the CDTI by the flight crew (P1.4). The flight crew then confirms approach parameters. Once the traffic is identified the flight crew notifies ATC via an acquisition message(P1.5). If for some reason the traffic can not be identified on the CDTI, the flight crew notifies ATC of an unsuccessful search (P1.6). An unsuccessful search is assumed to result in another attempt through processes P1.3, P1.4, and P1.5. If the search continues to be unsuccessful, it is assumed that the approach spacing procedure is abandoned, and that normal ATC guidance is provided. This is indicated by the dashed line leading to "revert to standard ATC ops."

If the identification process is successful, the crew will be provided with a spacing target by ATC or by an automated lookup based on the weight category of own ship and the lead ship (P1.7).

At this point in the procedure, ATC will provide a clearance to the flight crew to proceed (Phase 2). The flight crew then enters the "conduct approach spacing phase," (P3), and begins to follow speed guidance cues provided on the CDTI (P3.1). Meanwhile, ATC is expected to continue monitoring the aircraft approach to determine if an unsafe situation

is developing (P3.2). The flight crew simultaneously monitors the situation and responds to any alerts issued by the approach spacing system.

If a separation below the minimum wake vortex separation standards is detected by the airborne approach spacing system, an alert is issued to the flight crew and a breakout command is issued. Likewise, if ATC detects an unsafe situation, a command to breakout may be issued by a controller (P3.3). Based on commands from either ASIA or ATC, the flight crew performs a breakout maneuver (P3.4).

If the flight crew follows the guidance provided by the approach spacing system, and that guidance is within tolerance, appropriate spacing will be maintained through the approach, and phase 4 of the operation, completing the procedure, can proceed. In this case, a clearance for landing is issued by ATC (P4.1), followed by the crew flying the approach at the final approach speed and landing (P4.2). As part of phase 4, ASIA continues to monitor separation (P4.4) and if inadequate spacing is detected, the crew is alerted and may execute a missed approach (P4.3). Note that no active guidance is issued by the approach spacing system after the final approach fix; a command to decelerate to the final approach speed is given at the final approach fix, and it is expected that the flight crew will follow their planned final approach speed through the remainder of the approach..(Once the flight crew is at the final approach fix small speed changes may be made by the flight crew at their discretion).

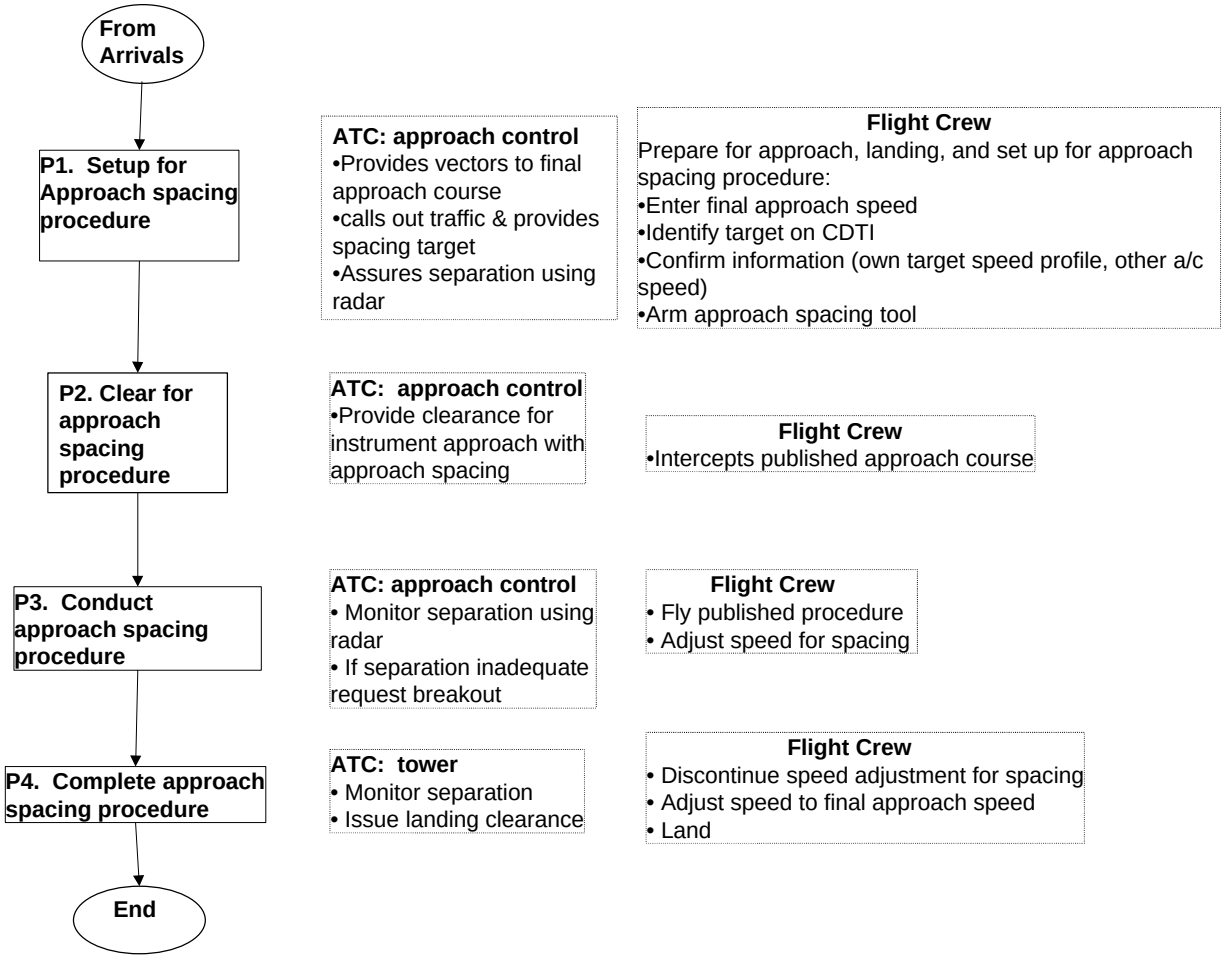

Figure 1. Approach Spacing Phases

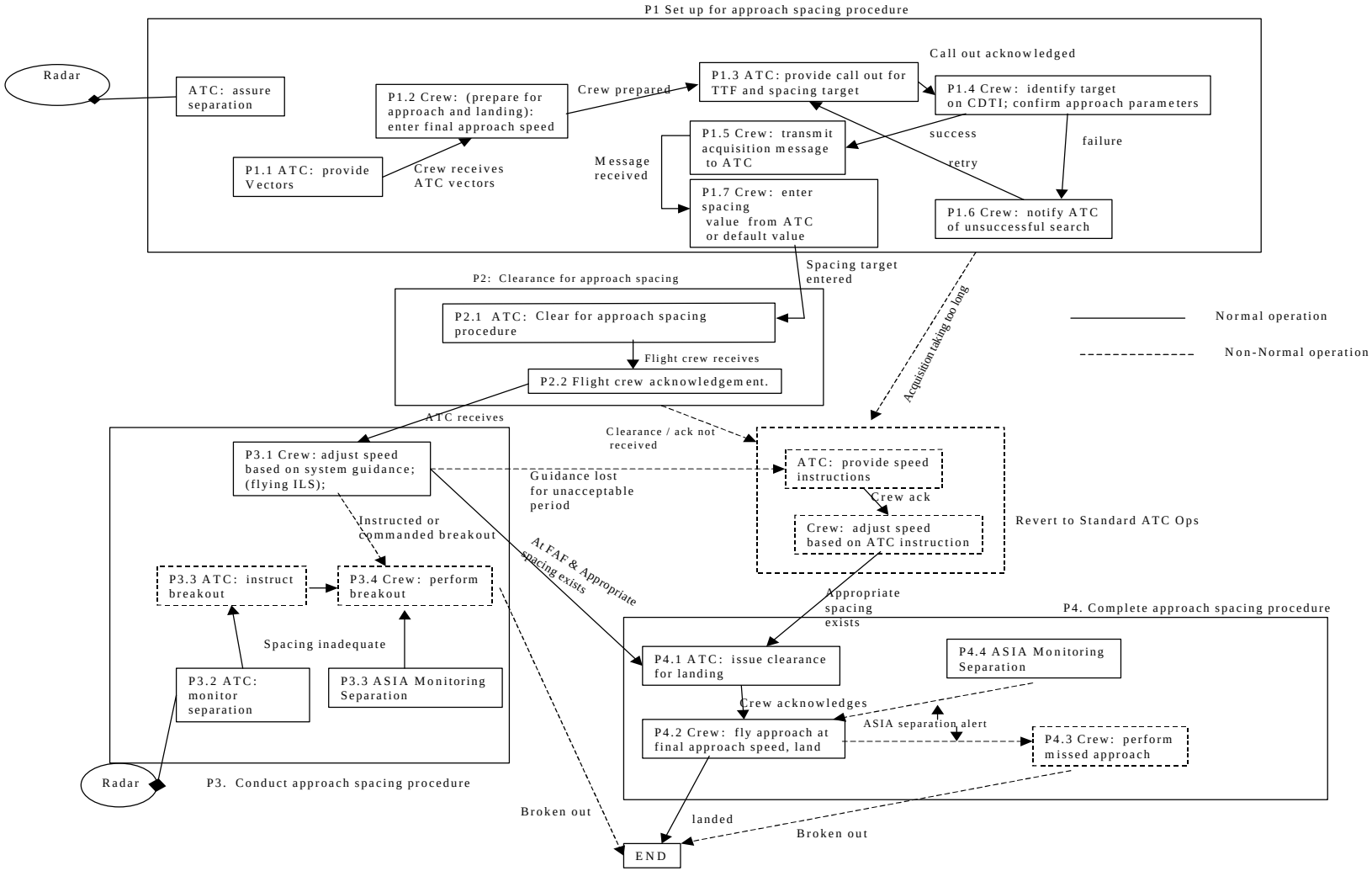

Figure 2. Approach Spacing Processes

D.1.2.2 Hazard and Safety Analysis

D.1.2.2.1 Operational Hazard Analysis (OHA)

The hazard analysis for ASIA consists primarily of a careful examination of the phase and process diagrams illustrated above in Figure 1 and Figure 2. Hazards are identified for each process depicted in Figure 2 by posing two hypotheses:

1. The process does not complete normally.
2. The process completes based on erroneous information or assumptions.

These two hypotheses form the basis of the hazard analysis that is presented in Table 2 below. Each hazard is identified with a unique number relating to the phase and process to enable reference.

The most significant hazards with ASIA are those that related to the identification of the lead aircraft as well as speed and those pertaining to phase 3, where flight crews are conducting the ASIA procedure. Consequently, these hazards drive the analysis requirements.

Table 2 contains the following columns:

- Phase (corresponding to the phases in Figure 1).
- Process (corresponding to the processes identified in Figure 2).
- OH number: This column lists the numeric designator that was assigned to each hazard. The form of the hazard identifier is: H.Phase.process.hazard_number.
- Operational Hazard description
- Potential Operational Consequence: The operational effect of encountering the identified hazard. Identifying the potential consequence (effect, failure condition) aids in determining the appropriate hazard class. Note, however, that a consequence of a hazard is not necessarily immediate. A series of events and combinations of hazards is normally required for a consequence to ultimately occur. This series of events and hazards are identified through a fault tree analysis that is documented in §D.1.2.2.3 below. This safety analysis also includes, as a potential mitigation, the intervention of ATC; ATC is expected to intervene if necessary to help prevent a mid-air collision.
- Environmental considerations (from Table 1): These are environmental and procedural considerations, assumptions, expectations, and requirements from the OSED that play a role in the operational hazard classification.
- Hazard Class: The classification of the operational hazards according to the severity of their identified consequences (effects, failure conditions) per the classification scheme. The class indicated corresponds to the worst possible effect. For example, impact of “erroneous approach speed” has been determined to potentially lead to wake vortex encounter (class 2 hazard) or mid-air collision with lead aircraft (class 1 hazard). Classification for this failure case is documented with the most severe consequence: class 1.

The objectives and requirements derived from the OHA for each hazard with a classification of 3 or higher (more hazardous) are further assessed as part of the ASOR process.

Some of the hazards have no further safety requirements and are not analyzed or allocated herein. The hazards that are not specifically related to the new services considered in this document and that remain unchanged from current operational procedures are not assessed; these hazard classification for these hazards is designated N/A (not applicable), since their safety assessment already forms part of the current operations and is subject to continuous monitoring. The hazards that were classified as 5 have no safety impact and are not further analyzed. Hazards that were classified as 4 are allocated “Minimum” requirements. Per AMJ 25.1309 §8b(2), “if the hazard assessment, based on experienced engineering judgment, determines that system malfunctions cannot result in worse than Minor Failure Conditions, or affect other airworthiness-related functions, no further safety analysis is necessary to show compliance with JAR 25.1309”.

Per AMJ 25.1309, no further analysis is necessary when the allocated requirements are ”Minimum”. However, in this end-to-end context, “system” should be interpreted as the “end-to-end system” encompassing both airborne and ground systems, and their supporting networks. For the airborne system, per RTCA DO-178B/Eurocae ED-12B §2.2.2, this safety requirement implies that the contribution of software components to these potential failure conditions must be mitigated by at least a software level D requirement. Similarly, this “minimum” safety objective applies to the ground system and the supporting network.

Table 2. Operational Hazard Analysis Results

Phase	Process	Hazard ID	Operational Hazard Description	Potential Operational Consequence	Environ-mental Consid-erations (from Table 1)	Hazard Class
P1: Setup	P1.1 (ATC provides vectors)	H1.1.1	No vectors provided by ATC	Identical to current operational procedure	N/A	N/A
	P1.2 Crew: prepare for approach and landing; enter final approach speed	H1.2.1	No approach speed entered	Procedures accommodate mixed equipage. Effect is equivalent to ASIA function not available with potential slight increase in workload	OE1/2 OO2/3 RG5 RA6/7	4
		H1.2.2	Erroneous approach speed entered	Wake vortex encounter Mid-air collision with lead a/c	RA1/2/4/6/7	1
	P1.3 ATC: provide callout for traffic to follow	H1.3.1	Erroneous traffic call out	Wake vortex encounter Mid-air collision with lead a/c	RG5 RA7	1
		H1.3.2	Loss of traffic call out	Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3 RG5 RA6/7	4
	P1.4 Crew: Identify target on CDTI	H1.4.1	Lead target traffic not found by crew	Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3 RG5 RA1/6/7	4
		H1.4.2	Lead traffic misidentified by crew	Wake vortex encounter Mid-air collision with lead a/c	RG5 RA7	1
	P1.5 Crew: transmit acquisition	H1.5.1	Loss of acquisition message	Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3 RG5 RA6/7	4
		H1.5.2	Erroneous acquisition message	Environment ensures that this is equivalent to loss of ASIA (H1.2.1) Note : this case is not related to erroneous lead traffic (H1.4.2)	OE1/2 OO2/3 RG5 RA6/7	4

Phase	Process	Hazard ID	Operational Hazard Description	Potential Operational Consequence	Environ-mental Consid-erations (from Table 1)	Hazard Class
P1: Setup	P1.6 Crew: notify ATC of unsuccess-ful search	H1.6.1	Loss of notification of unsuccessful search	Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3 RG5 RA6/7	4
		H1.6.2	Erroneous notification of unsuccessful search by crew	Environment ensures that this is equivalent to loss of ASIA (H1.2.1) Note : this case is not related to erroneous lead traffic (H1.4.2)	OE1/2 OO2/3 RG5 RA6/7	4
		H1.6.3	Delayed notification of unsuccessful search by crew	Environment ensures that this is equivalent to loss of ASIA (H1.2.1) Note : this case is not related to erroneous lead traffic (H1.4.2)	OE1/2 OO2/3 RG5 RA6/7	4
	P1.7 ATC: provide Spacing target, crew, enter spacing target	H1.7.1	Spacing target not received	Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3 RG5 RA6/7	4
		H1.7.2	Spacing target miscommunication	Wake vortex encounter Mid-air collision with lead a/c	OE1/2 OO2/OO4 RG5 RA6/7	1
		H1.7.3	Crew fails to enter spacing target	ASIA fails to engage; Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3 RG5 RA6/7	4
		H1.7.4	Crew enters incorrect spacing target	Wake vortex encounter Mid-air collision with lead a/c	OE1/2 OO2/OO4 RG5 RA6/7	1
P2: Clearance for procedure	P2.1 Controller issues clearance	H2.1.1	Loss of clearance for ASIA	Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3 RG5 RA6/7	4
	P2.2 Flight crew accepts clearance	H2.1.2	Erroneous clearance for ASIA	Environment ensures that this is equivalent to loss of ASIA (H1.2.1) Note : this case is not related to an erroneous ASIA clearance (H1.4.2)	OE1/2 OO2/3 RG5 RA6/7	4
		H2.2.1	Loss of flight crew acknowledgement of clearance for ASIA	Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3 RG5 RA6/7	4

Phase	Process	Hazard ID	Operational Hazard Description	Potential Operational Consequence	Environ-mental Consid-erations (from Table 1)	Hazard Class
		H2.2.2	Erroneous acknowledgment of ASIA clearance by flight crew	Environment ensures that this is equivalent to loss of ASIA (H1.2.1) Note : this case is not related to an erroneous ASIA clearance (H1.4.2)	OE1/2 OO2/3 RG5 RA6/7	4
P3: Conduct Procedure	P3.1 Crew: adjust speed based on system commands	H3.1.1	Erroneous speed maintained by flight crew	Wake vortex encounter Mid-air collision with lead a/c	OE1/2, O2/OO4, RG5, RA6/7	1
		H3.1.2	Loss of guidance during ASIA procedure	Environment ensures that this is equivalent to loss of ASIA (H1.2.1)	OE1/2 OO2/3/4 RG5 RA1/6/7	4
		H3.1.3	Erroneous guidance during ASIA procedure	Wake vortex encounter Mid-air collision with lead a/c	OE1/2, OO2/4, RG5, RA6/7	1
	P3.2 ATC: monitor separation	N/A		Identical to current operational procedure	N/A	N/A
P3: Conduct Procedure	P3.3 ATC: instruct breakout	N/A		Identical to current operational procedure	N/A	N/A
	P3.4 Crew: perform breakout	N/A		Identical to current operational procedure	N/A	N/A
P4: Complete approach spacing procedure	P4.1 ATC: issue clearance for landing	N/A		Identical to current operational procedure	N/A	N/A
	P4.2 Crew: fly final approach speed and land	N/A		Identical to current operational procedure	N/A	N/A
	P4.3 Crew: execute missed approach	H4.3.1	Unnecessary missed approach due to ASIA	Environment ensures that this is equivalent to loss of ASIA (H1.2.1). The major impact is on performance since unnecessary missed approach is conducted.	OE1/2, OO2/4/5 RG5, RA6/7	4 Note
		H4.3.2	Missed approach necessary but not started	Wake vortex encounter Mid-air collision with lead a/c	OE1/2 OO2/4/5	1

Note: Although hazard 4.3.1 leads to minor impact from a safety perspective, go around procedures adversely impact the efficiency of operations. Therefore, "nuisance" go around resulting from failures

associated with hazard 4.3.1 should be limited since the impact is that the ASIA function does "not perform its intended function".

The following four sections explain the rationale for the entries in Table 2.

D.1.2.2.1.1 Setup: Phase 1 Hazards of ASIA

The process of providing vectors (P1.1) is considered to be identical to current procedures and there is no new reliance on the ASA equipment to complete this part of Phase 1 of ASIA. Therefore no new hazards are identified for this part of the procedure, and this part of the operation is assumed to be safe.

Process 1.2 is a new process that is associated with ASIA. The hazards of non-completion or incorrect completion of the flight crew entry of final approach speed, identified in hazard 1.2.1, are analyzed. The process would not be completed if the flight crew were to not complete entry of the final approach speed. In this case the CDTI user interface and ASSAP must be coordinated to detect that no entry has been made, and to disable any further processing (RA6). Because of the radar controlled environment (OE1), the single stream approach operation (OE2) and the mixed equipage design (OO3), the procedure must be aborted and reversion to standard procedures (RA7/RG5) takes place. This will not create unsafe conditions since minimum spacing must be achieved prior to the lead aircraft crossing the threshold (OO2).

In the case where process 1.2 is completed based on erroneous information (hazard 1.2.2), it is assumed that the most likely reason is due to an incorrect flight crew entry of the planned final approach speed (RA4/7), although this is also possible due to an airborne system internal failure (RA1/2). An incorrect entry could possibly result in wake vortex separation standards being violated, or even eventually lead to a mid-air collision if corrective actions are not taken. Based on the analysis to be presented below, however, a mid-air collision can be avoided with high probability by using appropriate error checking in ASSAP and/or the CDTI. A wake vortex separation violation is mitigated by use of an ASIA separation monitoring function.

Hazards 1.3.1 and 1.3.2 are associated with the callout for traffic to follow (TTF) from ATC. Hazard 1.3.1 results from a miscommunication or misunderstanding of the correct traffic to follow (RG5, RA7). In this case the flight crew selects the wrong traffic. Specific outcomes of such a mistake are very scenario dependent but in the worst case either wake vortex separation minima or a mid-air collision could result. The fault-tree analysis assesses the risk of such an outcome.

Hazard 1.3.2 results if the intended target is never communicated. In this case the procedure must be aborted. Similar to the system response to hazard 1.2.1, in this case the CDTI and ASSAP must work together, with perhaps a time-out mechanism, to disable the provision of guidance when there is no target identified. With the same assumptions on the environment (OE1/2, OO2/3, RG5, RA6/7), this hazard can lead to the same consequences as hazard 1.2.1.

Hazards 1.4.1 and 1.4.2 are associated with the process of identifying the target on the CDTI. Hazard 1.4.1 occurs if the lead traffic is not found; in this case, the procedure must be aborted. This hazard can be related to the flight crew failing to identify the target (RA7) or the airborne system failing to display the aircraft (RA1/6). The impact can be limited to reverting to standard procedures with the same assumptions on the environment (OE1/2, OO2/3, RG5, RA6/7) as for hazard H1.2.1. Hazard 1.4.2 results when the lead traffic is misidentified (RG5, RA7), in which case the potential consequences are the same as with hazard 1.3.1, namely, possible wake vortex separation minima violation or mid-air collision. ASA equipment may play a direct role, however, in producing hazard 1.4.2; therefore, these hazards are included in further analysis of the potential operational consequences.

Hazards 1.5.1 and 1.5.2 result when the flight crew communication back to ATC that the target has been successfully acquired does not get through or is corrupted. In this case, both hazards result in the same outcome as hazard H1.2.1 with the same environment assumptions (OE1/2, OO2/3, RG5, RA6/7): the procedure is aborted. The incorrectly communicated acquisition message has the same result as a no communication; if ATC does not get a clear indication that the target has been identified, no clearance to proceed can be issued to the flight crew.

Hazards 1.6.1, 1.6.2, and 1.6.3 result when an unsuccessful search is not communicated or is communicated incorrectly. In the case where the communication is not received, the clearance to proceed can not be issued and reversion to standard procedures is necessary. Likewise, for a misunderstood communication, if ATC does not get a clear message that a successful target search has been completed, the assumption must be that the search was unsuccessful and the ASIA procedure is to be abandoned. These hazards result in the same outcome as hazard H1.2.1 with the same environment assumptions (OE1/2, OO2/3, RG5, RA6/7): the ASIA procedure is aborted and aircraft is instructed to revert to the standard approach procedure.

Hazard 1.6.3 results when the search is taking too long. As depicted in Figure 2, the net result is reversion to standard procedures.

Hazards 1.7.1, 1.7.2, 1.7.3, and 1.7.4 result when a failure of the spacing target communication occurs. As identified in the table, this can occur in one of four ways; first, if the spacing target is not received (H1.7.1) or the flight crew does not enter the target (H1.7.3), the procedure must be abandoned. These hazards result in the same outcome as hazard H1.2.1 with the same environment assumptions (OE1/2, OO2/3, RG5, RA6/7): the ASIA procedure is aborted and aircraft is instructed to revert to standard approach procedure. Likewise, the ATC to flight crew communication could be corrupted (H1.7.2), resulting in an incorrect target being entered. Alternatively, the information could be communicated correctly but then entered incorrectly by the flight crew (H1.7.4). In either hazard 1.7.2 or 1.7.4, the result can be a wake vortex separation minima violation or a mid-air collision.

D.1.2.2.1.2 Clearance for Approach Spacing: Phase 2 Hazards of ASIA

Phase 2 of the procedure consists of two steps – the issuing and the acceptance of the clearance for the flight crew to proceed to follow the automated guidance from the ASA systems. The possible hazards that are identified with these processes are that (H2.1.1) the clearance from ATC is lost, (H2.1.2) the clearance from ATC is misunderstood, (H2.2.1) the acknowledgement from the flight crew is not received, and (H2.2.2) the acknowledgement from the flight crew is misunderstood. If the clearance or acknowledgement is misunderstood it is effectively equivalent to non-receipt. In any of these cases once again reversion to standard procedures is required. These hazards may result in a small increase in workload for both the controllers and flight crews but the increase is assumed to be of minor criticality, and therefore these hazards are not further examined in this study.

D.1.2.2.1.3 Conduct Approach Spacing: Phase 3 Hazards of ASIA

Phase 3 of the ASIA procedure depends to a large extent on the ASA equipment. This is the most critical phase from the perspective of ASA requirements and it is examined in significant detail in the later sections. The primary process that is of interest to this analysis is the use of the equipment by the flight crew for speed guidance during the approach (P3.1).

Hazard 3.1.1 takes place if the flight crew does not follow the speed guidance; in this case a wake-vortex separation minima violation or a mid-air collision is possible.

Hazard 3.1.2 results if the guidance is lost during the procedure. This can occur due to detected ASA equipment failures, and is avoided by requiring minimum equipment continuity (RA1, RA6). If automated airborne guidance is lost, ATC is expected to provide guidance through the rest of the approach, as is done without ASIA.

Hazard 3.1.3 results when the ASIA system provides incorrect guidance to the flight crew. This hazard can result in wake vortex encounter or eventually a mid-air collision. The fault-trees resulting from this hazard are examined in detail in later sections along with additional supporting analysis.

Hazards related to processes P3.2 where ATC monitors aircraft approaches and P3.3 where ATC issues a breakout instruction are unchanged from current operations. Therefore no new hazards are identified for this part of the procedure, and this part of the operation is assumed to be safe.

Hazards 3.4.1 and 3.4.2 are a lack of or improper execution by the flight crew of a breakout when instructed or commanded by ATC. As there is no difference from existing procedures, there is no safety

degradation in executing a missed approach with ASIA. Therefore no new hazards are identified for this part of the procedure.

D.1.2.2.1.4 Completion of Approach Spacing: Phase 4 Hazards of ASIA

Phase 4 of the procedure requires the flight crew to fly a normal approach and landing. Although no active guidance is provided by ASIA during this operational phase, ASIA continues to monitor spacing. If the minimum spacing is broken an alert is generated an alert is generated. If the crew determines that it can not recover from the spacing error, a missed approach may be executed.

The only hazards that occur during this phase that are different from current procedures are when the crew performs a missed approach based on incorrect information from ASIA's alerting. Hazard 4.3.1, therefore, is an unnecessary missed approach due to ASIA. This hazard is not considered as a safety issue; therefore, it is not analyzed in the fault trees.

Hazard 4.3.2, is a missing alert when one is necessary. This hazard can result in wake vortex encounter or eventually a mid-air collision. The fault-trees resulting from this hazard are examined in detail in later sections along with additional supporting analysis.

D.1.2.2.2 Failure-Mode Analysis

The failure mode matrix shown as Table 3 is intended to provide a check list to be sure that all potential failures are covered in the hazard and fault tree analysis. Failures are listed for both systems and information elements. The fault tree analysis that follows incorporates each of the errors or failures listed in the table that are specific to the actual application. At least one relevant fault-tree figure is provided in the third column for reference purposes.

Table 3. Failure Mode Matrix

Required Information Element or System	Failure or Error	Relevant Figure(s) from Fault-tree analysis
ADS-B	System failure resulting in persistent error	Figure 4
TIS-B	System failure resulting in persistent error	Figure 4
ASSAP	System failure resulting in erroneous information	Figure 4
CDTI	System failure resulting in erroneous information	Figure 4
Navigation (lead)	Integrity failure	Figure 5
Navigation (trail)	Integrity failure	Figure 4
State Vector	Misleading information	Figure 4
Planned final approach speed	Wrong approach speed	Figure 7
Planned separation	Incorrect communication or entry	Figure 7
ID entry	Incorrect entry	Figure 6
Ground surveillance and automation	System failure	Figure 11, Figure 12

D.1.2.2.3 Fault Tree Analysis

The two potential operational consequences that are of significant criticality that are identified above in the hazard analysis are:

1. Wake vortex encounter
2. Mid-air collision.

ICAO procedures for ILS approaches are specifically designed on the basis of numerical risk based on the Collision risk model (ICAO doc 9274) . As one of the potential risks on such an ILS approach, a wake-vortex encounter, i.e., an encounter that can cause a serious aircraft upset, is considered to be a severe-major failure requiring a probability less than the order of 10^{-7} per operation. A mid-air collision is considered catastrophic; and the probability is required to be less than the order of 10^{-9} per operation.[1]

It is the purpose of this section to present a fault tree analysis of these two operational consequences in order to derive some ASA system requirements. The fault-tree analysis includes consideration of the

[1] This analysis was completed based on the assumption that the approach spacing application will last approximately 15 minutes. This is based on an assumption of a 30 nmi final approach segment flown at a speed of 125 knots.

earlier hazard analysis of §D.1.2.2.1. The relevant hazards as described in §D.1.2.2.1 are accounted for in this analysis. Table 4 below repeats the hazards from Table 2 that have relevance to either of these two operational consequences, and indicates the figure in the fault tree analysis below in which these hazards are treated. It is important to recognize that an operational hazard may appear at any level within the fault tree, depending on the events that contribute to that hazard, i.e., the hazard may be a leaf event itself, or an intermediate gate in the fault tree that is contributed to by more basic events.

Table 4. Operational Hazard Mapping to Fault Trees

Phase	Process	Hazard ID	Operational Hazard Description	Relevant Figure from Fault Tree Analysis
P1: Setup	P1.1 (ATC provides vectors)	H1.2.2	Erroneous approach speed entered	Figure 7 Figure 8 (Note)
	P1.3 ATC: provide callout for traffic to follow	H1.3.1	Erroneous traffic call out	Figure 6
	P1.4 Crew: Identify target on CDTI	H1.4.2	Lead traffic misidentified by crew	Figure 6
	P1.7 ATC: provide Spacing target, crew, enter spacing target	H1.7.2	Spacing target miscommunication	Figure 7
		H1.7.4	Crew enters incorrect spacing target	Figure 7
P3: Conduct Procedure	P3.1 Crew: adjust speed based on system commands	H3.1.1	Erroneous speed maintained by flight crew	Figure 4
		H3.1.3	Erroneous guidance during ASIA procedure	Figure 4
P4: Complete approach spacing procedure	P4.1 ATC: issue clearance for landing	H4.3.2	Missed approach necessary but not started	Figure 3

Note: Hazard 1.2.2 can occur on either the lead ship or the trail ship; this is identified in the fault-trees that follow below.

As discussed in §D.1.2.2.1, several of the hazards identified in the hazard analysis do not lead to high criticality operational consequences and are considered to be more of a concern from an operational viability perspective, e.g., hazards 1.4.1, 1.6.3, and 4.3.1. Hazard 4.3.1 is considered as a failure of the system in its intended function and is treated in a later section.

D.1.2.2.3.1 Fault Tree Analysis of Wake Vortex Encounter

The fault-tree analysis begins with an examination of the likelihood of a wake vortex encounter during an approach. Figure 3 presents the high-level fault tree for this occurrence. The purpose of the figure and the associated analysis and requirements described below is to substantiate one possible solution (ASOR) to achieve the required 10^{-7} per hour maximum (order of magnitude) failure rate. The second level of Figure 3 represents a selected allocation of requirements. The values for "OP/SYS ERRORS" and "W/V SEPARATION ALERT" are determined bottom-up by subsequent analysis in Figure 4 and Figure 9 .

This analysis provides one possible solution for the allocation of requirements in order to comply with the limit for the required maximum failure rate. This analysis provides one mean of achieving the high-level safety requirement by selecting one combination of system requirements. However, it is recognized that other combinations of system requirements could be selected in order to achieve the same goal.

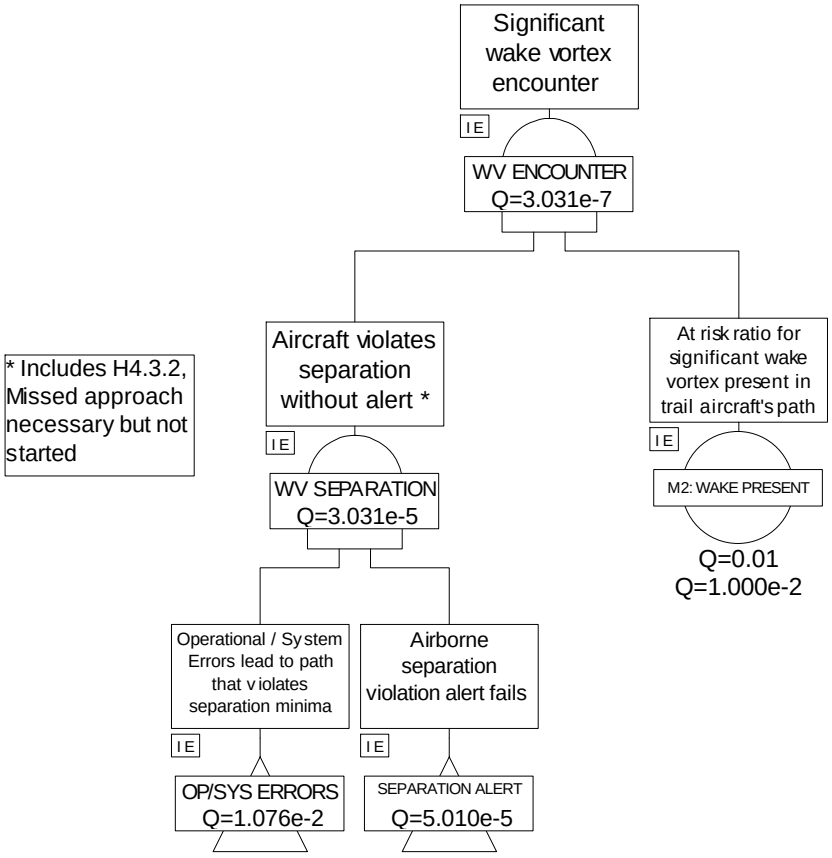

Figure 3. High Level Fault Tree for Wake Vortex Encounter Analysis

The wake vortex encounter can occur only when the trail aircraft violates the separation minima and there is a wake present to upset the aircraft (depicted by the top AND gate in the fault-tree). Since the ASIA system is designed to avoid wake vortex separation violations, a significant separation violation only occurs if there are unexpected system or operational errors and an airborne violation alert (RA6) fails.

This analysis assumes no mitigation due to air-traffic control. The reason for this is that the analysis assumes that wake vortex encounter could take place shortly after a separation violation; it is assumed that ATC has no responsibility to notice the violation. Therefore, the responsibility for avoiding a wake vortex separation violation is assumed to be on the airborne side, i.e., via airborne alerts generated by ASIA.

Another important assumption is the probability of a wake being in the trail aircraft's path (the "at risk ratio"). Our assumption is that the wake vortex separation that the flight crews have to maintain is numerically equal to the separation that air-traffic control currently has to maintain on approach. When inside these minima, which occurs typically today during visual approaches, a possibility of a wake vortex encounter is assumed. The probability of the encounter, however, is somewhat uncertain. Due to the uncertainty of this event, a very conservative number of 10^{-2} was adopted. This assumption was not validated analytically but was derived based on interviews with line pilots, experienced in flying visual approaches well below the current IMC wake vortex separation standards. The consensus of the flight crews who discussed this was that 10^{-2} is an extremely conservative assumption**. It is noted, however, that this is one key assumption of the analysis that will probably need further validation before certification / operational approvals for ASIA can take place.**

The assumption on the risk ratio results in a requirement that operational and system errors be held to 10^{-5} or lower. This value is achievable through a combination of system requirements on guidance, error checking, and alerting. It is necessary to have an alert for separation violations, as shown in the figure, as a mitigation to other potential system failures. The failure sub-trees for the operational/system errors and the alert are further analyzed below. The analysis now proceeds to work down through more detailed levels of the fault tree, working from left to right through the sub-trees of Figure 3.

Note that the overall probability of the AND gate labeled "WV Separation" does not equal the multiplicative probability of the two gates below it; this is because the two gates feeding this AND gate are not independent (they contain "common mode" failures).

D.1.2.2.3.1.1 Operational and System Errors Leading to Wake Vortex Encounter Path

Figure 4 shows the fault-tree for the left-most branch of Figure 3. This branch considers operational and system errors that could potentially lead to a flight path that violates wake vortex separation minima.

Two operational hazards are identified at the second level of this fault-tree. First, there is a possibility that the flight crew (Hazard H1.4.2) has misidentified the traffic; second, the system may provide misleading guidance to the flight crew (Hazard H3.1.3).

D.1.2.2.3.1.1.1 Misidentification of Lead Traffic

Consider the possibilities that may lead to traffic misidentification. First, a significant, persistent error in the state vectors for the lead traffic might result in another target being selected. Second, the trail ships' navigation system may have errors that result in a similar effect. Third, an incorrect target ID might have been conveyed to the flight crew or the flight crew may inadvertently select the wrong target (identified as Hazards H1.3.1 and H1.4.2). Finally, the CDTI or ASSAP sub-systems may malfunction in a way that causes the misidentification.

Working down to the fourth level on the left-hand side of Figure 4, a persistent state vector error may be caused by a persistent error in the ADS-B system, or an undetected lead ship navigation integrity failure.

A persistent error in ADS-B or TIS-B reports is presumed to have a probability on the order of 1 in 10^{-5} per flight hour. Proposed ADS-B messaging and cyclic redundancy coding (CRC) coding schemes provide a single message error rate of no more than this order, and generally a much lower order. The 10^{-5} value assumes a combination ADS-B hardware and software errors, and error correction coding.

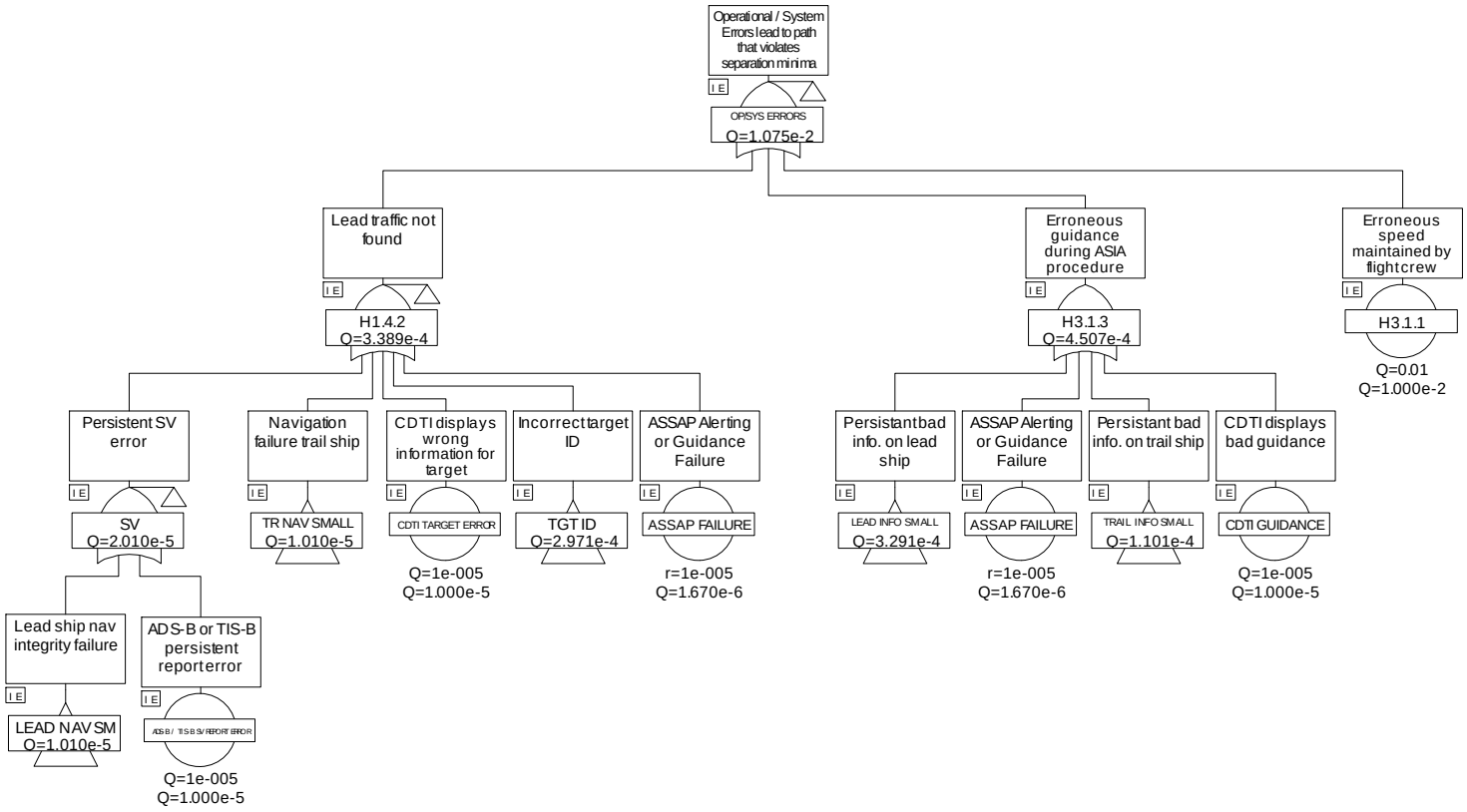

Figure 4. Operational / System Errors Lead to Path That Violates WV Separation Minima

Figure 5 illustrates the sub-tree for a lead-ship navigation integrity failure. In this tree there are two bottom level events: an integrity failure of the lead ship and an area-wide navigation integrity failure. The single ship failure represents an integrity failure of the lead ships' on board navigation system. This failure is assumed to take place with a per operation rate of 10^{-5}. An area navigation failure is a common mode failure with the trail ship, and the same failure will be included in the trail ship's fault tree. An area

navigation failure affecting both the lead and trail ship is assumed to occur with a frequency that is two orders of magnitude lower than a single ship failure, i.e., with a per operation rate of 10^{-7}. This is consistent with signal in space integrity requirements for GPS WAAS and LAAS (see ICAO Annex 10, Table A2-4). The total of the lead ship's navigation system integrity failure results in a per operation rate of 1.01×10^{-5}.

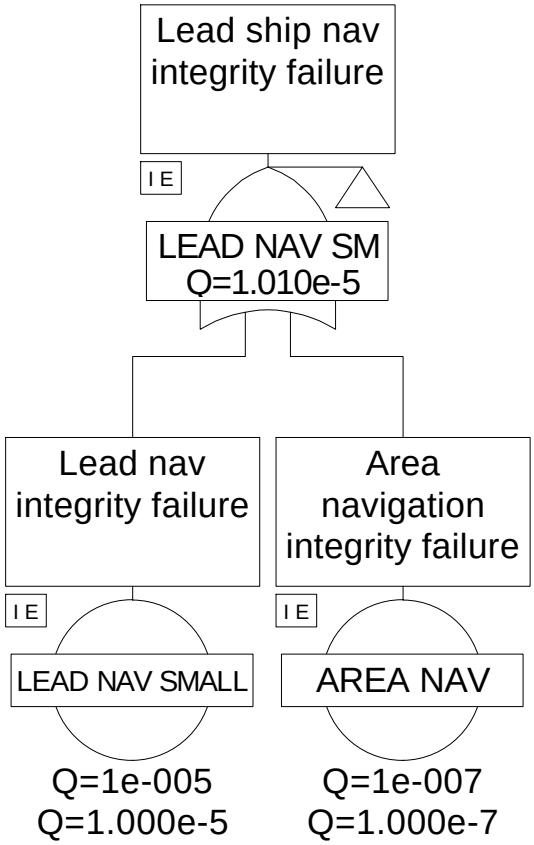

Figure 5. Fault Tree for Navigation Integrity Failure of Lead Ship

Figure 6 illustrates the fault tree for an incorrect target ID. It is assumed that a crosscheck is performed by the flight crew when the target ID is entered. Therefore, an incorrect target ID is propagated when there is an incorrect initial entry and the crosscheck fails. An incorrect entry takes place when incorrect data is entered into the system, through mistaken entry of the flight ID, selection of the wrong target, or through miscommunication. Miscommunication takes place on the controller side, on the flight crew side, or due to the communications system corrupting the data. Our assumptions are that communications system failures resulting in a miscommunication are on the order of 10^{-5} per flight hour, and that a human error is on the order of 10^{-2} per communication, as per the (introductory material reference).

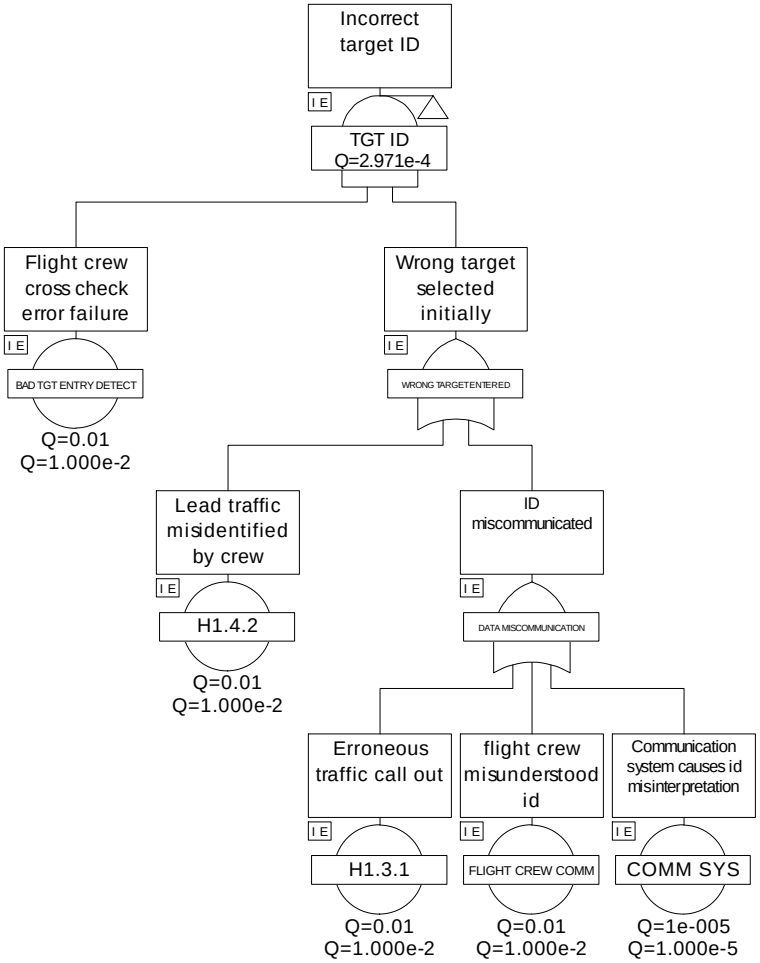

Figure 6. Incorrect Target ID

D.1.2.2.3.1.1.2 Misleading Guidance

The right hand side of the tree in Figure 4 shows four basic failures that would result in misleading guidance (hazard H3.1.3). These are persistent bad information on the lead ship or persistent bad information on the trail ship. In addition, a CDTI or ASSAP failure is also considered to potentially lead to this hazard.

That the bad information must be persistent is self-evident and is stated here as a requirement: temporarily corrupted data should not lead to guidance that will cause a violation of wake vortex separation minima. By temporary we mean any time epoch less than that which is required for the separation minima to be violated.

The next section examines the fault trees for persistent misinformation for the lead and trail ships.

D.1.2.2.3.1.1.2.1 Persistent Misinformation for the Lead Ship

Figure 7 identifies the three major causes of persistent misinformation for the lead ship. First, an error in the lead plan data that is communicated to the trail ship will result in persistent misinformation. Second, a persistent error in the state vector information transmitted by the lead ship to the trail ship is considered. Third, if the controller provides or the flight crew enters an incorrect spacing target, or if an automated entry by ASIA is in error, and is below the wake vortex separation minima for the lead/trail weight category combination, the possibility of a wake vortex separation violation exists.

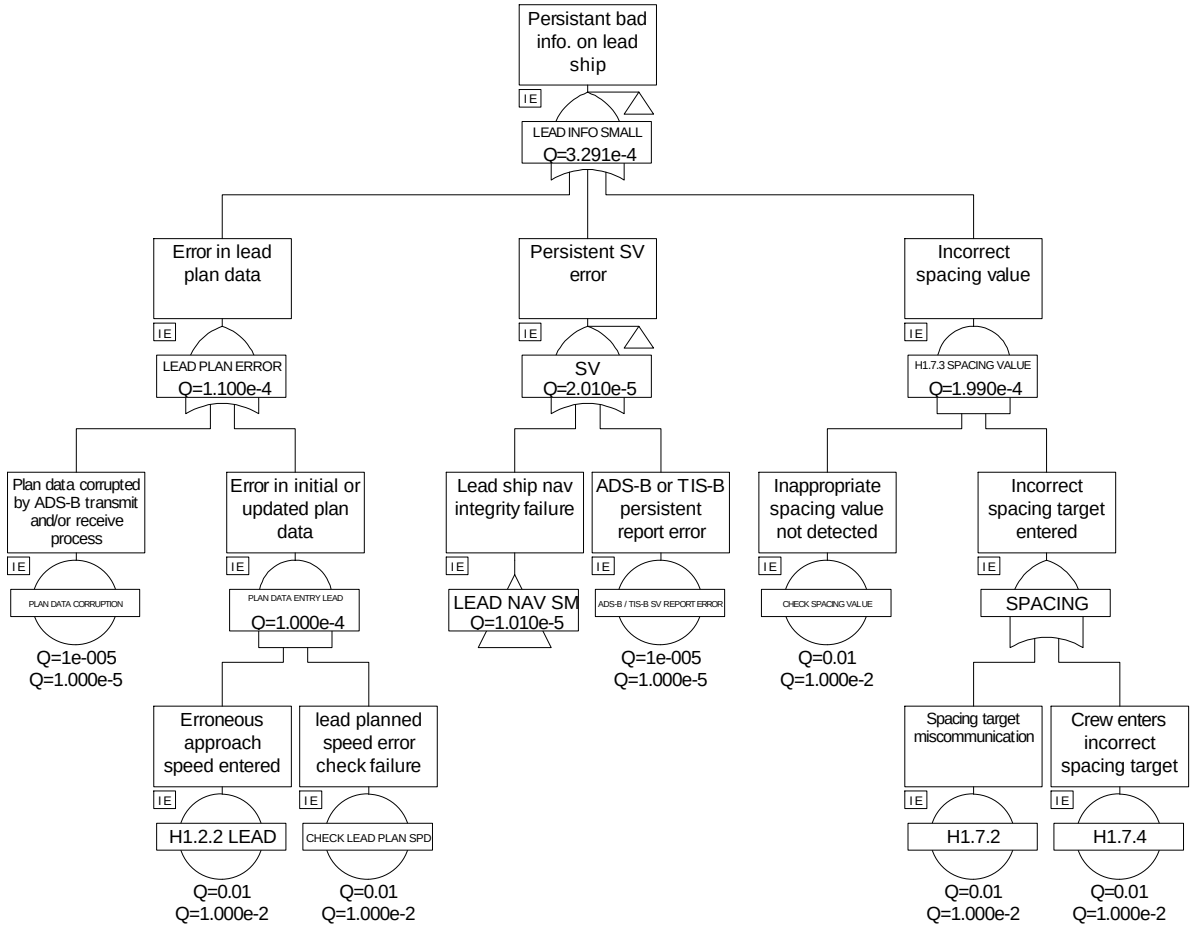

Figure 7. Fault Tree for Persistent Bad Information for Lead Ship

Error in Lead Plan Data

An important potential source of incorrect information is the planned final approach speed that must be manually entered into the system during Process 1.2. The event labeled H1.2.2, representing the hazard identified with Process 1.2, is a data entry error by the flight crew of the lead aircraft. This error is assumed to occur with a failure rate of 1 per 100 approaches. Given this large failure rate due to human input, an identified requirement is that error checking be performed by the crew; in addition, it is useful to put in place automation to detect gross errors in the input. While no credit is taken in the fault tree for any automation of the error checking, error checking is listed as a requirement, because it should be possible to detect gross errors in this input, (e.g., errors that are greater than 50 or 100 knots).

It is conceivable that a small input error that is undetected by error checking could lead to a wake vortex separation minima violation. Sensitivity analysis to the failure rate of the error check found that the overall probability of a significant WV encounter is insensitive to this parameter. Much of the credit for this insensitivity lies with the required alert for a separation violation.

The combination of the input error and a failure in the input error check leads to the gate labeled “plan data entry lead.” A possible error in the message transmission process that could lead to a separation violation, labeled as the event “plan data corruption,” is also included with an assumed failure rate of 1 in 10^{-5} approaches.

Persistent SV Error

Moving to the right in Figure 7, consider a persistent state vector error as another source of misinformation that can lead to a wake vortex separation minima violation. The sources of a state vector error were described in detail in section 4.1.1.1.

Incorrect Spacing Target

Finally, bad information might be connected with an inappropriate spacing target being entered by the flight crew, either due to miscommunication with ATC or due to an input error. This error should be readily detectable; hence, an error check is required on this input, although it is not considered in the fault tree.

D.1.2.2.3.1.1.2.2 Persistent Misinformation for the Trail Ship

The fault tree presented in Figure 8 represents the failures that can result in persistent misinformation for the trail ship. The tree is very similar to that of the lead ship, minus the additional possible failures that result from transmission/reception problems. The trail ship also must input a final approach speed that is used in the calculation of speed guidance for the approach, therefore, a parallel input error and error check is considered for the trail ship fault tree.

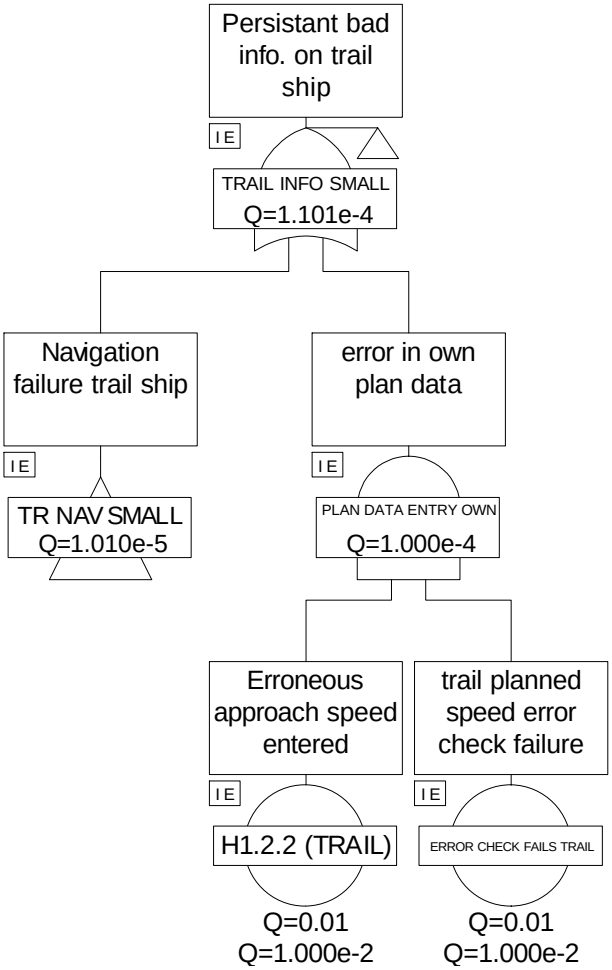

Figure 8. Fault Tree for Persistent Bad Information for Trail Ship

D.1.2.2.3.1.2 Airborne Separation Violation Alert Fails

Reexamining Figure 3, observe that an essential mitigation to a wake vortex separation minima violation is that the violation is detected by on-board systems. It is an assumption of this analysis that when such a violation is detected an alert is issued to the flight crew and that the minimum separation is promptly reestablished. We assume that this sequence of events will avoid a wake vortex encounter provided that the alert is issued before a large violation of the wake vortex minima takes place. Precise values for this minimum detection interval and the sensitivity of the detection to the navigation integrity will be discussed in a later section.

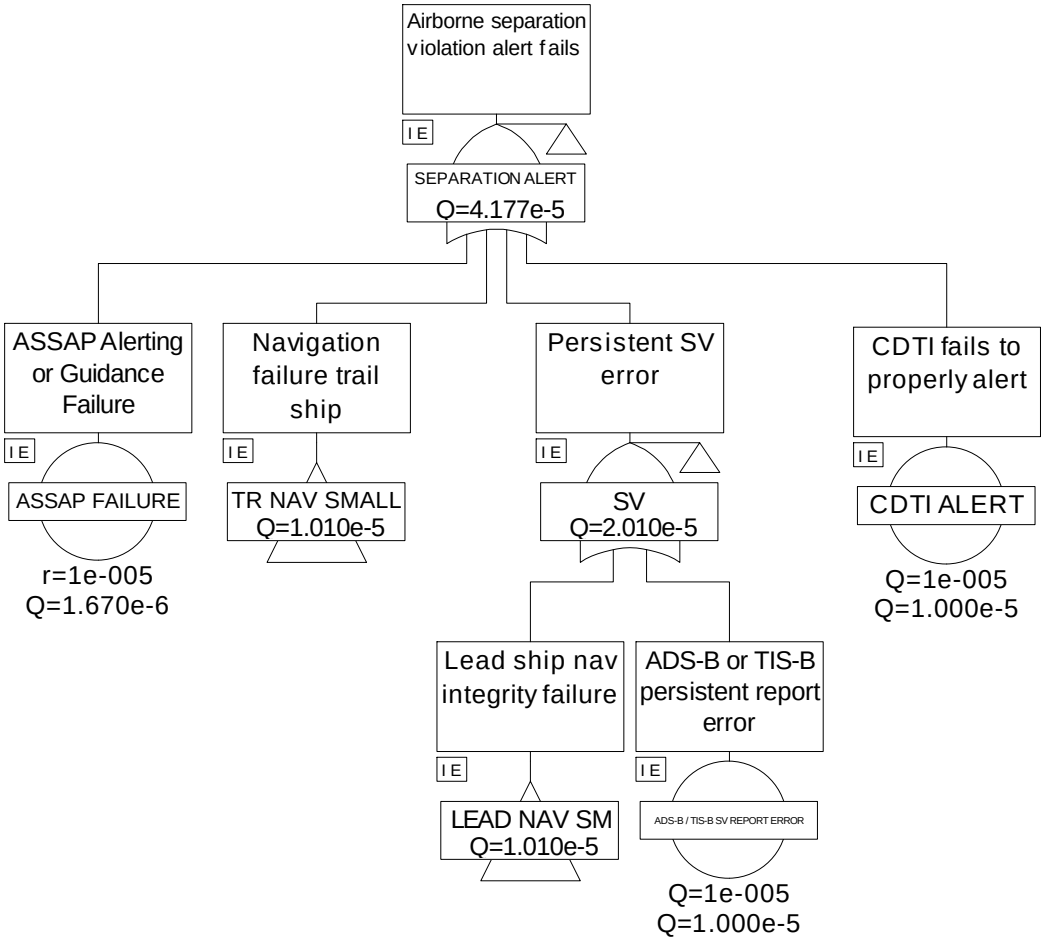

Figure 9. Fault Tree for Airborne Separation Violation Alert Failure

The fault tree of Figure 9 illustrates the failure mechanism for the airborne separation violation alert. The alert is based on current position estimates for both the lead and trail aircraft; the primary source of failure is state vector information from the lead aircraft and navigation information from the trail aircraft. In addition, the analysis considers a failure of the alerting algorithm itself, presumed to occur with a 10^{-5} failure rate. The state vector and navigation integrity failures are common mode failures with the operational and system errors considered in Section 4.1.1. These common mode failures are included in the calculation of the top-level event of a wake vortex encounter shown in Figure 3.

Navigation Integrity Containment Requirements

While the fault tree analysis presented above provides a reasonable way to establish required failure rates for navigation integrity, it does not provide an analytic basis on which to set the required navigation containment limit. To provide some insight into the effects of various navigation containment integrity bounds, a Monte-Carlo simulation was used that employs an approach spacing algorithm that has been tested and confirmed to achieve results reasonably compatible with the operational goals of ASIA. That algorithm is not documented in this appendix; rather, the intent is that a final algorithm will be documented as part of the ASSAP MOPS requirements.

In any case the Monte-Carlo simulation models the aircraft approaches, approach spacing guidance, and pilot responses to the guidance inputs. The simulation also models an alerting algorithm that is triggered if the aircraft violate wake vortex separation minima.

For this particular study, the simulation was run with false information in the final approach speed plan data that is supplied to the trail aircraft. The false information is construed such that the trail aircraft is misled that the lead aircraft final approach speed will be much greater than is actually planned. This causes the trail aircraft to be issued guidance that results in frequent separation violations.

The analysis modeled a navigation integrity error as a position bias error just below the specified navigation integrity bound in the Monte-Carlo model. The direction of the error was uniformly distributed and selected at random at the beginning of each approach. Our metric in evaluating various navigation integrity containment bounds was the cumulative probability distribution of the distance inside the wake vortex separation minima at which the violation was actually detected. The integrity containment bounds were selected to correspond with the navigation integrity category (NIC) levels specified in RTCA DO-242A (ADS-B MASPS).

Figure 10 shows the results of this analysis. The figure shows the probability of detecting the wake-vortex separation violation (the ordinate) as a function of true distance inside the wake separation minima (the abscissa). Three values of navigation integrity category were examined; the integrity category [ref DO242A] and the associated containment radius (Rc) are indicated in the figure.

As expected, detection probability degrades as a function of increasing containment radius. The 75 m containment radius performs best, with all detected violations occurring within 1000 ft of the separation minima. At Rc=185 m the detected violations are within 2000 ft of the minima, and with Rc=370 m some violations are not detected until between 2500 ft and 3000 ft of the minima. The suggested containment boundary is 75 m, as it appears to be reasonably assured that this will help to minimize the likelihood of a wake vortex encounter. The 75 m containment radius can mostly likely be met by differentially corrected GPS such as WAAS. This value represents best engineering judgement. It is feasible that a lower NIC can be used with the same safety level at the cost of some reduction in overall system performance (reduced throughput) by adding extra buffer to the spacing target.

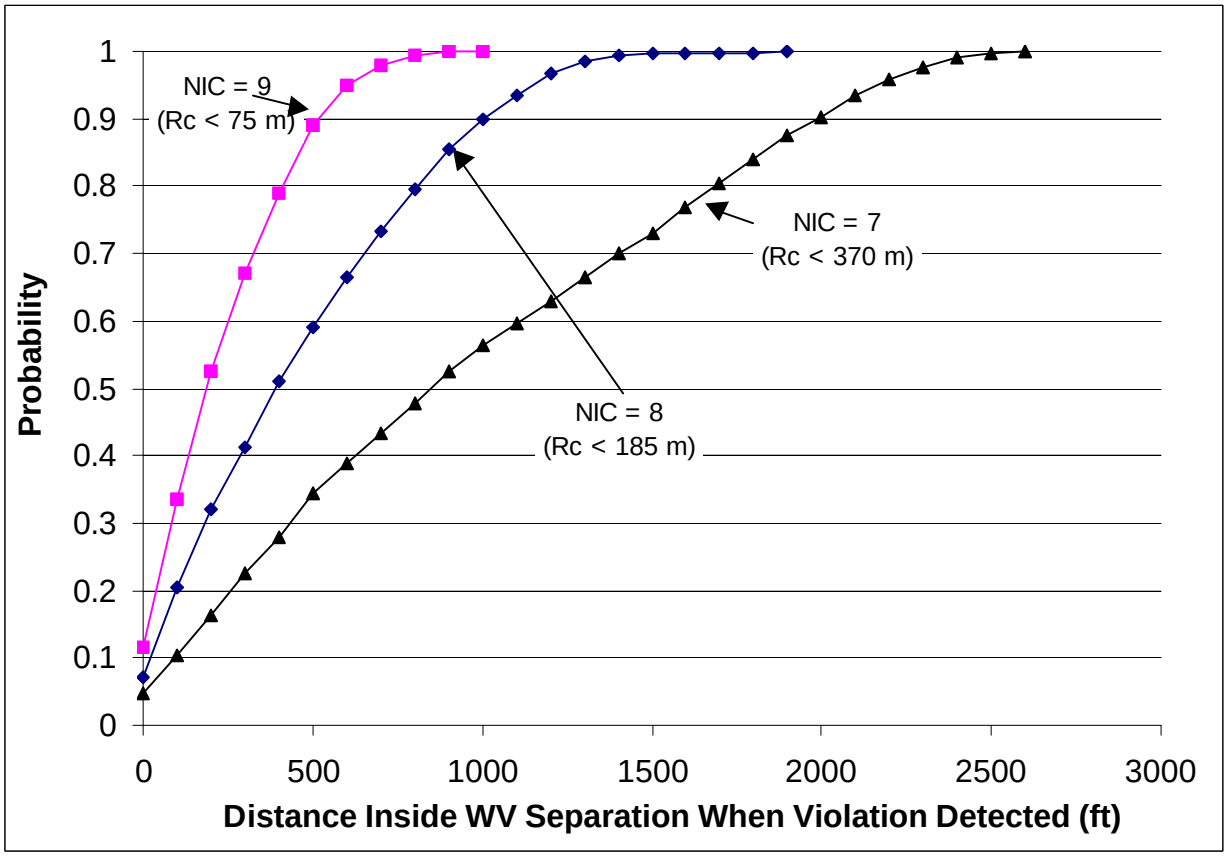

Figure 10. Sensitivity of WV Violation Detection to Navigation Containment Bound

D.1.2.2.3.1.3 Summary of Wake Vortex Encounter Analysis

This section completes the analysis of the likelihood of a wake vortex encounter. We conclude that if the bottom level events occur at or below the rates described in the fault trees drawn above, the overall rate of a wake vortex encounter will be held to the 10^{-7} order of magnitude. This is an acceptable criticality (severe-major) for a wake vortex encounter.

For wake avoidance, we recommend an operating NIC of 9 (75 m containment radius) and a SIL of 2 (10^{-5} or better undetected navigation integrity failure rate).

D.1.2.2.3.2 Fault Tree Analysis of Mid-Air Collision with Lead Aircraft

This section analyzes the risk of a mid-air collision between the trail aircraft and the lead aircraft[2].

We conduct a risk analysis of a mid-air collision based on two different assumptions for the information that is supplied to ATC. Although the baseline procedure as articulated earlier in this appendix assumes utilization of secondary surveillance radar (SSR), it is of importance to also examine the case where both airborne and ATC surveillance is provided by ADS-B. The fault tree of Figure 11 shows the assessment when air traffic control surveillance is supported by SSR. Figure 12 contains a fault tree for the case where both air traffic control and airborne surveillance are provided by ADS-B. In the case where both ATC and airborne separation assurance are based on a common source of information, a common failure mode exists that must be accounted for in the analysis.

[2] The risk of a mid-air collision with another aircraft not involved in the approach is not addressed in this analysis. It is assumed that since the approach procedure is typical, that there is no introduction of additional collision risk with another aircraft beyond that of standard procedures that are considered acceptable today.

Figure 11 is essentially identical to Figure 3, with a wake-vortex separation violation being replaced with a collision path. In addition, Figure 11 includes an additional failure of ATC to notice and correct the problem. The ATC component is introduced because it is expected that ATC will step in if a gross violation is noticed. It is not expected that ATC will be responsible for separation, other than to monitor and to help avoid a collision in the exceedingly rare situation that the aircraft are on a collision path. The hazards and failures leading to a collision path are identical to those that lead to a wake vortex separation violation; the difference is in the magnitude of the failure.

Figure 11 assumes that ATC continues to rely on secondary radar for monitoring the situation. In contrast, Figure 12 considers a case where ATC uses ADS-B information. Since ADS-B represents a possible eventual replacement for SSR, as a part of the probe analysis, it is useful to examine the requirements that would be necessary with such a surveillance architecture. Other than surveillance integrity, Figure 12 assumes the same hazard and event likelihoods as Figure 11. Table 5 shows the resulting mid-air collision probabilities as a function of the undetected navigation failure rate. The table indicates that an order of magnitude more navigation integrity will be needed for the case where ADS-B is the sole source of surveillance information (note that the results indicated in Figure 12 are based on a 10^{-7} integrity). Note that it is the navigation subsystem integrity, and not the other subsystem integrity levels that need to be boosted for the sole-means case.

Table 5. Mid-Air Collision Rate vs. ATC Surveillance Source

Airborne surveillance	ATC Surveillance	Navigation Integrity Undetected Failure Rate (per flight hour)	ASIA Mid-Air Collision Rate (per operation)	Acceptable Collision Risk
ADS-B	SSR	10^{-5}	10^{-12}	Yes
ADS-B	ADS-B	10^{-5}	10^{-8}	No
ADS-B	ADS-B	10^{-7}	10^{-9}	Yes

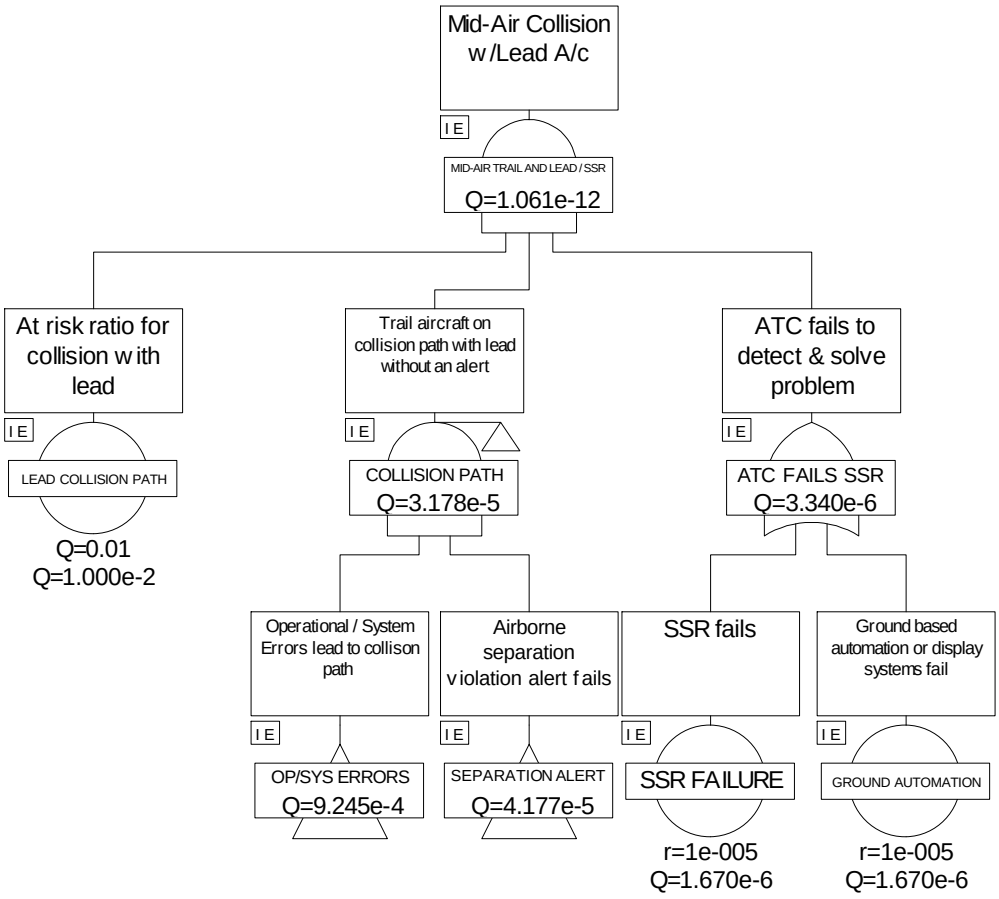

Figure 11. Top Level Fault Tree for Mid-Air Collision with Lead; ATC based on Secondary Surveillance Radar

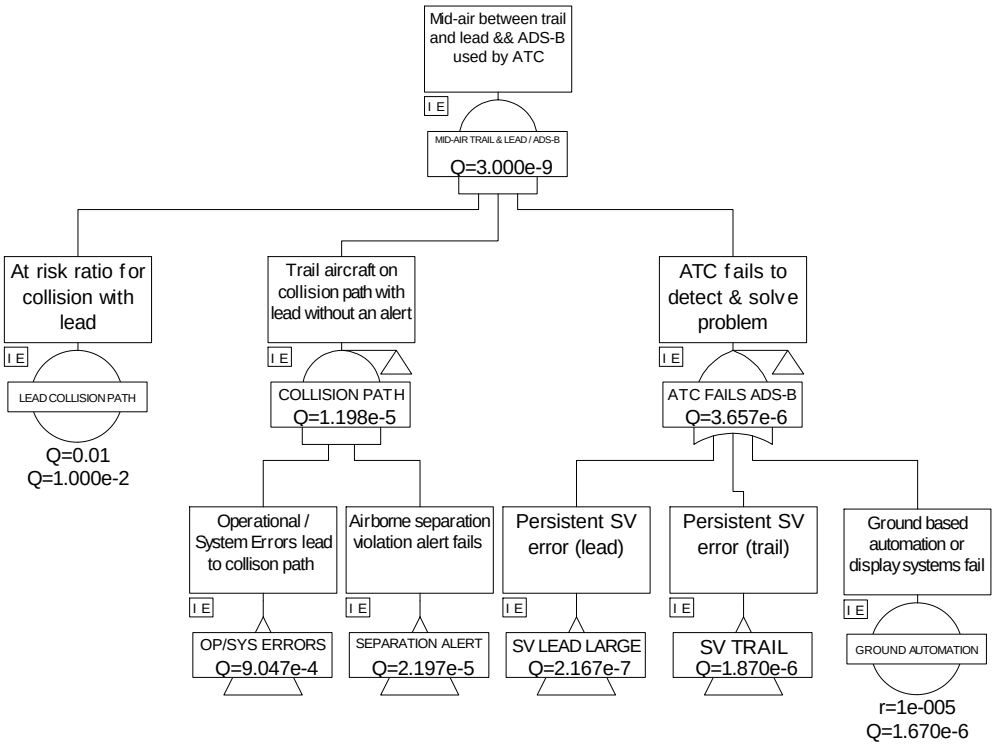

Figure 12. Top Level Fault Tree for Mid-Air Collision with Lead; ATC based on ADS-B

As we expect that SSR will be available for a considerable time period, a 10^{-5} integrity is initially acceptable to run ASIA operations. Ultimately, if ADS-B becomes the sole surveillance source for both ATC and airborne applications, it may be necessary to have the navigation information achieve a 10^{-7} integrity. It is, however, possible that this analysis has been overly conservative in assuming the same probability for a small integrity error leading to a wake vortex minima separation violation as for a large error leading to a collision. If it can be substantiated that an integrity error of enough magnitude to cause a collision is less likely (by two orders of magnitude), then it may be possible to reduce the 10^{-7} requirement back to 10^{-5}.

D.1.2.3 Analysis of Requirements Supporting Intended Function of ASIA

The ASIA application is intended to increase runway throughput without increasing missed approaches. A Monte-Carlo simulation that includes a model of the surveillance environment, a model for the guidance algorithm, and a model for the flight crew response to guidance inputs was employed in order to assess requirements supporting ASIA. The simulation models wake vortex separation minima for large, heavy, and small aircraft. This analysis assumed a mix of 12% heavy, 8% small, and 80% large aircraft.

The simulation models multiple arrivals in a single stream approach. The number of aircraft arrivals is selected, then Monte-Carlo simulations are achieved by running multiple instances of the arrival stream. Statistics are collected on the overall throughput at the runway threshold, the average separation and inter-arrival time as a function of arrival number, and the number of go-arounds. It is assumed that each time the wake vortex separation minima are broken, a go-around is issued.

Since the primary purpose of ASIA is to improve runway throughput, the simulation was set up such that deliveries to the approach stream were at an average rate of about 37 per hour, including all aircraft weight categories. The details of the simulation are presented in [ref Wang, Hammer]. The average rate of 37 per hour represents an improvement of between 4 and 5 arrivals per hour over what our simulation indicates can be with the traffic mix that is specified above.

The objective of these simulation runs was to determine surveillance requirements for update rate, position and velocity accuracy, and latency. The analysis was conducted by determining acceptable baseline values for these parameters, then degrading selected parameters to see where acceptable performance is no longer achieved. The process was methodical; the resulting requirements are sufficient and reasonable, but no claims are made that the requirements are necessary, or that they are in any way optimal.

The metric of this study is the number of actual separation minima violations that are recorded for every 1000 approaches. Generally about 25,000 approaches were run for each result. The minima violations were broken into two categories: the total violations and those that were 1,000 feet or more below the separation requirement considered “significant.” Our assumption is that a “significant” violation is likely to result in a go-around whereas a technical violation of less than 1,000 feet below the minima will result in a minor but annoying disruption and increased workload for the flight crew and possibly the controllers. A limit was set of a rate of 1 per 1,000 approaches of significant violations and 2 per 1,000 approaches of total violations.

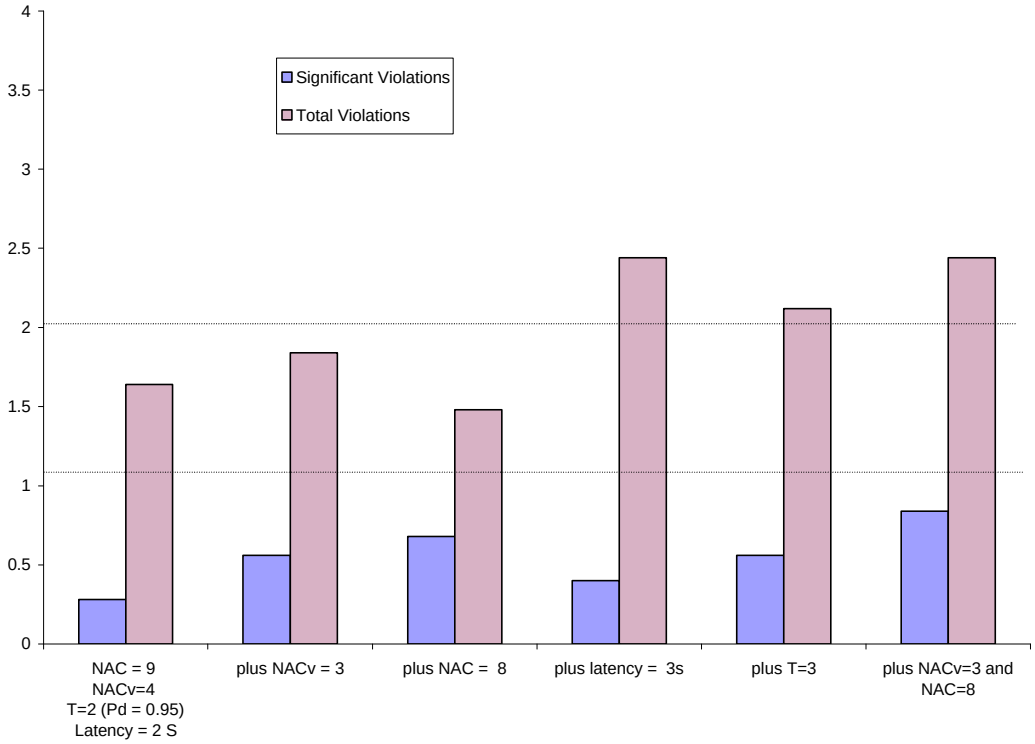

Figure 13. Baseline of NAC=9, NACv=4, T=2 S, Latency = 2S with Variations

Figure 13 illustrates the results of these experiments. The figure shows a baseline result on the left hand side that is augmented by various reductions in performance in the examples to the right. Figure 13 illustrates that with NAC=9, NACv=4, a latency of 2 seconds, and an update period of 2 seconds with a 95% success rate, that the desired operational performance is achieved. Degrading either latency or update period to 3 seconds results in unacceptable performance in terms of total violations. Degrading NAC to 8 or degrading NACv to 3 still results in acceptable performance, but degrading both NAC to 8 and NACv to 3 causes the proportion of total violations to exceed the recommendation.

It is suggested, therefore, that a minimum requirement of NAC=9, NACv=4, update period of T=2 S with success probability of 0.95, and a latency of 2 seconds be the minimum requirements to initiate ASIA. Degradation of NAC to 8 or NACv to 3 during the procedure is considered acceptable to continue the operation.

System Continuity Requirements

While the safety analysis did not determine a need for a system continuity requirement for this application, the economic benefit of the application will depend on the system introducing very few missed approaches due to a continuity failure. The assumption being made is that no more than 1 in 1000 approaches should be allowed to be broken off, resulting in a continuity requirement of 99.9% per operation.

D.1.2.4 Requirements Summary

This section summarizes the requirements that have been derived in the sections above.

D.1.2.4.1 Data Requirements

Data requirements are as specified below.

Data Element Þ Performance Requirement ß	State Vector	Planned Final Approach Speed	Planned intermediate approach speeds & range from threshold[1]	Source of Requirement
Navigation Accuracy Category – Position (NACp)	NACp >= 8	N/A	N/A	D.1.2.3
Navigation Accuracy Category – Velocity (NACv)	NACv > 4 if NAC=8 NACv >3 if NAC>=9	N/A	N/A	D.1.2.3
Navigation Integrity Category (NIC)	NIC=9	N/A	N/A	D.1.2.2.3
System Integrity Level	10^{-5} 10^{-7} (desired if ADS-B is sole-source surveillance)	Corruption probability by system < 10^{-7}	Corruption probability by system < 10^{-7}	D.1.2.2.3
Maximum Delay to Indicate Integrity Changes	TBD	N/A	N/A	Best Engineering Judgement
Latency of Transmitting Information	≤ 2 sec	< 15 sec	Update within 5 seconds of a change[2]	D.1.2.3
Maximum Age of Applicability for Dynamic Data]	TBD	N/A	Update Within 5 seconds of a change[2]	D.1.2.3
Effective Update Rate	2 Seconds	N/A	N/A	D.1.2.3
Report Time Accuracy	0.1 Sec	N/A	N/A	D.1.2.3
Continuity	>99.9% per operation			D.1.2.3
Availability	No Requirement			No safety dependency found
Coverage	Approach corridor			D.1
Vehicle Participation	All Vehicles on Approach			D.1

D.1.2.4.2 Subsystem Integrity Requirements

Based on the fault-tree analysis of D.1.2.2.3, the Navigation, ADS-B (combination of transmitting and receiving subsystems), ASSAP, and CDTI subsystems need to maintain an integrity of 10^{-5} per flight hour.

D.1.2.4.3 Processing Requirements

1. A guidance algorithm is to be specified in ASSAP MOPS.
2. Temporarily corrupted state vector data should not lead to guidance that will cause a violation of wake vortex separation minima. The probability of a persistent error due to ADS-B < 10^{-7}.
3. A detection algorithm that alerts when wake vortex minima have been violated shall be provided.

D.1.2.4.4 Display requirements

Displays shall be provisioned to allow:

1. View of flight identification, horizontal position, and altitude of surrounding traffic;
2. Selection and highlight a specific target on the display;
3. Selection of the ASIA function;
4. Input the final approach speed for own aircraft and input the other aircraft flight identification and final approach speed as well as the desired minimum target spacing;
5. Arming the ASIA tool (if the tool set requires such a function);
6. Determining that the approach algorithm is operating normally;
7. Displaying lead aircraft information to assist in monitoring the longitudinal distance with the lead aircraft (e.g., ground speed, range read-out);
8. Determining / viewing the lead aircraft position for a safe interval;
9. Viewing and utilizing the ASIA tool (e.g., speed guidance) to assist in acquiring the target position;
10. Viewing when own ship has achieved minimum target spacing, not at minimum target spacing, and at a breakout point; and
11. Determining when the spacing task is to be discontinued.

In addition:

12. Provision shall be made for the flight crew to enter planned final approach speed into the approach spacing system through the CDTI. It is expected that an FMS will act as an interface to the CDTI so that the flight crew is able to enter the necessary parameters.
13. Provision shall be made for lead traffic identification and selection on the CDTI.
14. A check shall be provided on the separation entered versus weight category wake vortex separation minimums.
15. ASIA guidance shall not be enabled if no entry is made for planned final approach speed, lead traffic identification, or desired separation.
16. An error check on the flight crew entered planned final approach speed shall detect all errors above errors greater than 100 knots.

D.1.2.4.5 Assumptions

Assumptions are made on systems or personnel that are beyond the scope of the requirements in this document. Satisfactory system performance depends on the following assumptions:

Navigation:

Navigation systems are assumed to support the navigation accuracy and integrity described above.

Air Traffic Control:

1. It is assumed that controllers will have adequate tools to identify appropriately equipped aircraft (e.g., via flight strips, datablock).
2. It is assumed that ATC employs a conflict detection algorithm with 10^{-5} probability of failing to detect a violation of wake vortex separation minima.
3. It is assumed that the secondary surveillance radars fail with $< 10^{-5}$ probability per operation.
4. It is assumed controllers will take appropriate action when alerted to a violation of minimum separation standards.

Flight Crew:

It is assumed that flight crews will follow system guidance.

It is assumed that flight crews will take appropriate action when alerted to separation minima violation.